



Website Defacement Prevention Audit Checklist

20-Point Anti-Defacement Hardening Audit

- Are all admin users reviewed?
- Are dormant users deleted?
- Are passwords unique and strong?
- Is MFA enabled?
- Are login attempts limited?
- Are plugins updated?
- Are unused plugins/themes deleted?
- Are themes legitimate?
- Are file upload areas restricted?
- Are file permissions reviewed?
- Is FTP/cPanel secured?
- Are unsafe staging tools removed?
- Is file integrity monitoring active?
- Is a firewall configured?
- Is CDN bot filtering enabled?
- Are homepage uptime checks active?
- Are backups verified?
- Has restore been tested?
- Are SSL trust signals healthy?
- Is monthly website review scheduled?

Scoring:

17–20 = Strong anti-defacement maturity

12–16 = Moderate visible attack exposure

0–11 = High public vandalism vulnerability